

25.09.03

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日                      2 0 0 3 年    8 月 1 8 日  
Date of Application:

REC'D 13 NOV 2003

WIPO

PCT

出 願 番 号                      特 願 2 0 0 3 - 2 9 4 1 0 1  
Application Number:  
[ST. 10/C] :                      [ J P 2 0 0 3 - 2 9 4 1 0 1 ]

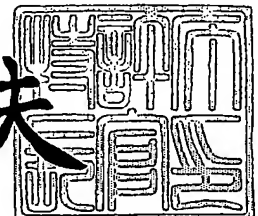
出      願      人                      F D K 株 式 会 社  
Applicant(s):

PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2 0 0 3 年 1 0 月 3 1 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康 夫



【書類名】 特許願  
【整理番号】 IP03533  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 7/58  
【発明者】  
    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケイ株式会社  
                        社内  
    【氏名】 山本 博康  
【発明者】  
    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケイ株式会社  
                        社内  
    【氏名】 中野 初美  
【発明者】  
    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケイ株式会社  
                        社内  
    【氏名】 清水 隆邦  
【発明者】  
    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケイ株式会社  
                        社内  
    【氏名】 アナンダ ビターナゲ  
【発明者】  
    【住所又は居所】 東京都港区新橋 5 丁目 3 6 番 1 1 号 エフ・ディー・ケイ株式会社  
                        社内  
    【氏名】 鯉渕 美佐子  
【特許出願人】  
    【識別番号】 000237721  
    【氏名又は名称】 エフ・ディー・ケイ株式会社  
【代理人】  
    【識別番号】 100096862  
    【弁理士】  
    【氏名又は名称】 清水 千春  
    【電話番号】 03-3543-0036  
【選任した代理人】  
    【識別番号】 100067046  
    【弁理士】  
    【氏名又は名称】 尾股 行雄  
    【電話番号】 03-3543-0036  
【手数料の表示】  
    【予納台帳番号】 057761  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1

## 【書類名】特許請求の範囲

## 【請求項 1】

抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを 2 個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて“0”または“1”を出力するフリップ・フロップを備え、

前記各積分回路に入力される入力信号の位相を調整するディレー、第 1 セレクターおよびアップ／ダウンカウンタからなる位相調整部を備え、

前記フリップ・フロップから出力される“0”または“1”がそれぞれ 50% に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、

前記各積分回路の前段にそれぞれ第 2 セレクターおよび第 3 セレクターを設け、

前記アップ／ダウンカウンタの最上位ビットによって前記第 1 セレクターと前記第 2 セレクターおよび前記第 3 セレクターとの入力の極性切換を行う極性切換回路を設けたことを特徴とする物理乱数発生器。

## 【請求項 2】

抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を 1 つ備え、

ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを 2 個ずつ備え、

前記各エッジ検出回路の出力信号の位相差に基づいて“0”または“1”を出力するフリップ・フロップを備えた物理乱数発生器において、

前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、

前記フリップ・フロップから出力される“0”または“1”がそれぞれ 50% に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けたことを特徴とする物理乱数発生器。

## 【請求項 3】

前記積分回路の抵抗の後段に FET を当該積分回路のキャパシタと並列に付加したことを特徴とする請求項 1 または請求項 2 に記載の物理乱数発生器。

## 【請求項 4】

前記積分回路の抵抗に代えて定電流回路を設けたことを特徴とする請求項 1 から請求項 3 までのいずれかに記載の物理乱数発生器。

## 【請求項 5】

請求項 1 から請求項 4 までのいずれかに記載の物理乱数発生器を 2 個以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリアル物理乱数に並べ替えて出力するようにしたことを特徴とする物理乱数発生装置。

【書類名】明細書

【発明の名称】物理乱数発生器および物理乱数発生装置

【技術分野】

【0001】

本発明は、各種の用途に用いるに好適な物理乱数発生器および物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（例えば、CG、自動作曲）、制御、計測、FA、ロボット制御（人工知能）などが挙げられる。

【背景技術】

【0002】

従来この種の物理乱数発生装置としては、例えば特許文献1に開示されているように、2個のディレーおよびセクター等からなる位相調整部と、フリップ・フロップと、フィードバック回路とから構成される物理乱数発生器を備えたものが知られている。

【特許文献1】特開2003-29964号公報

【発明の開示】

【発明が解決しようとする課題】

【0003】

しかし、これでは、フリップ・フロップのクロック端子とデータ端子に入力される2系統の信号ラインに応じた2個のディレーおよびセクターが必要となるので、位相調整部、ひいては物理乱数発生器の規模が大きくなり、その占有面積が拡大するばかりか、その消費電力が増大するという不都合があった。特に、物理乱数発生器がCPU（中央演算処理装置）、ROM（読取り専用記憶装置）、RAM（読取り書込み記憶装置）などの多くの機能とIC（集積回路）内に混載される場合には、この物理乱数発生器の占有面積をできる限り縮小することが強く望まれる。

【0004】

本発明は、このような事情に鑑み、占有面積が小さくて消費電力が少ない物理乱数発生器と、この物理乱数発生器が組み込まれた物理乱数発生装置を提供することを目的とする。

【課題を解決するための手段】

【0005】

まず、本発明のうち請求項1に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路と、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングするミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを2個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて“0”または“1”を出力するフリップ・フロップを備え、前記各積分回路に入力される入力信号の位相を調整するディレー、第1セクターおよびアップ／ダウンカウンタからなる位相調整部を備え、前記フリップ・フロップから出力される“0”または“1”がそれぞれ50％に収束するように当該フリップ・フロップの出力を前記位相調整部にフィードバックするフィードバック回路を備えた物理乱数発生器において、前記各積分回路の前段にそれぞれ第2セクターおよび第3セクターを設け、前記アップ／ダウンカウンタの最上位ビットによって前記第1セクターと前記第2セクターおよび前記第3セクターとの入力の極性切換を行う極性切換回路を設けて構成される。

【0006】

また、本発明のうち請求項2に係る発明は、抵抗およびキャパシタでクロック信号を積分して積分波形を出力する積分回路を1つ備え、ノイズ源と、このノイズ源のノイズを増幅してノイズ信号を出力するアンプと、前記積分波形と前記ノイズ信号とをミキシングす

るミキサーと、このミキサーの出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路とを2個ずつ備え、前記各エッジ検出回路の出力信号の位相差に基づいて“0”または“1”を出力するフリップ・フロップを備えた物理乱数発生器において、前記フリップ・フロップに入力される入力信号の位相を調整するディレーとセレクターからなる可変ディレーを前記各エッジ検出回路の前段または後段に設け、前記フリップ・フロップから出力される“0”または“1”がそれぞれ50%に収束するように当該フリップ・フロップの出力を前記可変ディレーにフィードバックするフィードバック回路を設けて構成される。

【0007】

また、本発明のうち請求項3に係る発明は、前記積分回路の抵抗の後段にFETを当該積分回路のキャパシタと並列に付加して構成される。

【0008】

また、本発明のうち請求項4に係る発明は、前記積分回路の抵抗に代えて定電流回路を設けて構成される。

【0009】

さらに、本発明のうち請求項5に係る発明は、上記物理乱数発生器を2個以上並列接続し、前記各物理乱数発生器に入力されたパラレル物理乱数をシリアル物理乱数に並べ替えて出力するようにして構成される。

【発明の効果】

【0010】

本発明のうち請求項1に係る発明によれば、ディレーおよび第1セレクターを半分にしてゲート数を削減することができるので、物理乱数発生器の規模を小さくして占有面積を縮小するとともに、その消費電力を低減することが可能となる。

【0011】

また、本発明のうち請求項2に係る発明によれば、2系統の信号ラインについて積分回路が1つで済むことに加えて、積分回路を構成する抵抗、キャパシタの誤差による位相調整範囲を狭めることができるため、可変ディレーを縮小し、ゲート数を削減することができることから、物理乱数発生器の規模を小さくして占有面積を縮小するとともに、その消費電力を低減することが可能となる。

【0012】

また、本発明のうち請求項3に係る発明によれば、積分回路のキャパシタに充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点、ひいてはジッターの分布を安定させ、良質な乱数を生成することができる。また、積分回路のキャパシタに充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間が短縮されることに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げるので、さらなる時間短縮が可能となることから、乱数生成スピードを大幅に高速化することができる。

【0013】

また、本発明のうち請求項4に係る発明によれば、積分回路を構成するキャパシタの充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みがなくなるため、乱数の質を向上させることができる。

【0014】

さらに、本発明のうち請求項5に係る発明によれば、複数の物理乱数発生器からなる物理乱数発生装置の乱数の質を向上させることができる。

【発明を実施するための最良の形態】

【0015】

以下、本発明の実施形態を図面に基づいて説明する。

【0016】

<第1の実施形態>

図1は本発明に係る物理乱数発生器の第1の実施形態を示す回路図、

図2は図1に示す物理乱数発生器のエッジ検出回路の詳細を示す回路図、  
図3は図1に示す物理乱数発生器の動作波形を示す図である。

【0017】

この物理乱数発生器1においては、図1および図3に示すように、抵抗Rおよびキャパシタ（コンデンサ）Cでクロック信号を積分して積分波形を出力する積分回路5と、ノイズ源6と、このノイズ源6のノイズを増幅してノイズ信号を出力するアンプ7と、積分波形とノイズ信号とをミキシングするミキサー8と、このミキサー8の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路9とが2個ずつ設けられている。各エッジ検出回路9は、図2に示すような回路構成となっており、これらのエッジ検出回路9の後段には、図1に示すように、各エッジ検出回路9の出力信号の位相差に基づいて“0”または“1”を出力するDタイプのフリップ・フロップ10が設けられている。さらに、フリップ・フロップ10の後段には、乱数をクロック信号に同期させるDタイプのフリップ・フロップ11が設けられている。

【0018】

また、物理乱数発生器1の最前段には、各積分回路5に入力される入力信号の位相を調整する位相調整部2が設けられており、この位相調整部2はディレー21、第1セレクター22およびアップ／ダウンカウンタ23から構成されている。

【0019】

また、フリップ・フロップ11の出力とアップ／ダウンカウンタ23との間にはフィードバック回路3が設けられており、フリップ・フロップ11から出力される“0”または“1”がそれぞれ50%に収束するようにフリップ・フロップ11の出力が位相調整部2にフィードバックされる。すなわち、フィードバック回路3は第1カウンタ31、比較器32、第2カウンタ33、レジスタ34、比較器35、シフトレジスタ／レジスタ36、加算器37から構成されており、第1カウンタ31および比較器32はフィードバックの周期を乱数（ $2 \times m$ ）で生成する。また、第2カウンタ33、レジスタ34および比較器35はフィードバックの周期（ $2 \times m$ ）中の“0”または“1”の数をカウント（n）し、比較データをアップ／ダウンカウンタ23に出力して乱数の一様性を補正するフィードバック信号を出力する。さらに、シフトレジスタ／レジスタ36および加算器37は、フィードバックの周期を決める乱数（m）を出力（OUT）より取得する。これにより、フィードバック周期による乱数の質の低下（癖）を防ぐことができる。

【0020】

さらに、位相調整部2と各積分回路5との間にはそれぞれ第2セレクター15および第3セレクター16が設けられているとともに、第1セレクター22とアップ／ダウンカウンタ23との間には極性切換回路13が設けられており、表1に示すように、アップ／ダウンカウンタ23の最上位ビットMSBによって第1セレクター22と第2セレクター15および第3セレクター16との入力の極性切換が行われる。

【0021】

【表 1】

アップ/ダウンカウンタ	SELECT	第1セクターのアドレス	第2セクターの出力	第3セクターの出力	相対的な時間差
1Fh 1Eh ⋮ ⋮ ⋮ 02h 01h 00h	1 ⋮ ⋮ 1 ⋮ ⋮ ⋮	1Fh 1Eh ⋮ ⋮ ⋮ 02h 01h 00h	0 (A) 0 (A) ⋮ ⋮ ⋮ 0 (A) 0 (A) 0 (A)	P-1 (A) P-2 (A) ⋮ ⋮ ⋮ 2 (A) 1 (A) 0 (A)	P P-1 ⋮ ⋮ ⋮ 3 2 1
3Fh 3Eh ⋮ ⋮ ⋮ ⋮ 22h 21h 20h	⋮ ⋮ ⋮ 0 ⋮ ⋮ ⋮ ⋮ ⋮	00h 01h 02h ⋮ ⋮ ⋮ ⋮ 1Eh 1Fh	0 (B) 1 (B) 2 (B) ⋮ ⋮ ⋮ ⋮ P-2 (B) P-1 (B)	-1 (B) -1 (B) -1 (B) ⋮ ⋮ ⋮ ⋮ -1 (B) -1 (B)	0 -1 -2 ⋮ ⋮ ⋮ ⋮ -P+2 -P+1

## 【0022】

したがって、2系統の信号ラインに応じた2個のディレーおよびセクターを必要とする従来の物理乱数発生器と比べて、ディレー21および第1セクター22を半分にしてゲート数を削減することができるので、物理乱数発生器1の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

## 【0023】

## ＜第2の実施形態＞

図4は本発明に係る物理乱数発生器の第2の実施形態を示す回路図である。

## 【0024】

この物理乱数発生器1においては、図4に示すように、抵抗RおよびキャパシタCでクロック信号を積分して積分波形を出力する積分回路5が1つ設けられているとともに、ノイズ源6と、このノイズ源6のノイズを増幅してノイズ信号を出力するアンプ7と、積分波形とノイズ信号とをミキシングするミキサー8と、このミキサー8の出力波形に基づいて生成されるジッターの最初のエッジを検出するエッジ検出回路9とが2個ずつ設けられている。これらのエッジ検出回路9の後段には、各エッジ検出回路9の出力信号の位相差に基づいて“0”または“1”を出力するDタイプのフリップ・フロップ10が設けられており、フリップ・フロップ10の後段には、乱数をクロック信号に同期させるDタイプのフリップ・フロップ11が設けられている。

## 【0025】

また、フリップ・フロップ10と各エッジ検出回路9との間（各エッジ検出回路9の後段）にはそれぞれ、ディレーとセクターからなる可変ディレー19が設けられており、フリップ・フロップ10に入力される入力信号の位相を調整することができる。

## 【0026】

さらに、フリップ・フロップ11の出力とアップ/ダウンカウンタ23との間にはフィードバック回路3が設けられており、フリップ・フロップ11から出力される“0”または“1”がそれぞれ50%に収束するようにフリップ・フロップ11の出力が可変ディレー19にフィードバックされる。

## 【0027】

したがって、2系統の信号ラインについて積分回路5が1つで済むことに加えて、積分回路5を構成する抵抗R、キャパシタCの誤差による位相調整範囲を狭めることができるため、ディレーとセクターからなる可変ディレー19を縮小し、ゲート数を削減することができることから、物理乱数発生器1の規模を小さくして占有面積を縮小し、その消費電力を低減することが可能となる。

## 【0028】

## ＜その他の実施形態＞

なお、上述した第2の実施形態において、図5に示すように、積分回路5の抵抗Rの後段にFET（電界効果トランジスタ）17をキャパシタCと並列に付加してもよい。この場合は、図6に示すように、積分回路5のキャパシタCに充電された電荷を放電して電位を積分波形の基点に戻すことにより、積分波形の基点が常に安定し、その結果としてジッターの分布も安定する。さらに、ジッターの分布が安定することは良質な乱数を生成することにつながる。また、乱数生成は電位が基点に戻るまで待たなければならないが、積分回路5のキャパシタCに充電された電荷が高速に放電され、電位も高速に積分波形の基点に戻るため、乱数生成までの待ち時間を短縮することができる。それに加え、乱数生成後に波形の電位が上がりきるのを待たずして強制的に基点まで電位を下げることもできるので、さらなる時間短縮が可能となる（乱数生成したら、すぐに電位を基点まで戻せる）。これにより、乱数生成スピードを大幅に高速化することができる。同様に、上述した第1の実施形態において、各積分回路5の抵抗Rの後段にFET17をキャパシタCと並列に付加することもできる。

## 【0029】

また、上述した第2の実施形態において、図7に示すように、積分回路5の抵抗Rに代えて定電流回路18を設けても構わない。この場合は、図8に示すように、キャパシタCの充電時の積分波形が直線となり、ノイズに対して変調したジッターの歪みなくなるため、乱数の質が向上する。同様に、上述した第1の実施形態において、各積分回路5の抵抗Rに代えて定電流回路18を設けることも可能である。

## 【0030】

また、図9に示すように、上述した物理乱数発生器1をk個（kは2以上）並列接続し、各物理乱数発生器1に入力されたパラレル物理乱数をk個のシリアル物理乱数に並べ替え、排他的論理和（XOR）素子を介して出力することにより、複数個の物理乱数発生器1からなる物理乱数発生装置の乱数の質を向上させることもできる。

## 【0031】

また、上述した第1および第2の実施形態においては、乱数発生用のフリップ・フロップとしてDタイプのフリップ・フロップを用いた場合について説明したが、本発明ではこれに限定されるわけではなく、これと同等の機能を有するフリップ・フロップであれば代用することができる。

## 【0032】

また、上述した第2の実施形態においては、図4に示すように、ディレーとセレクトーからなる可変ディレー19をエッジ検出回路9の後段に設けた場合について説明したが、可変ディレー19をエッジ検出回路9の前段に設けてもよい。

## 【図面の簡単な説明】

## 【0033】

- 【図1】本発明に係る物理乱数発生器の第1の実施形態を示す回路図である。
- 【図2】図1に示す物理乱数発生器のエッジ検出回路の詳細を示す回路図である。
- 【図3】図1に示す物理乱数発生器の動作波形を示す図である。
- 【図4】本発明に係る物理乱数発生器の第2の実施形態を示す回路図である。
- 【図5】積分回路の別の例を示す回路図である。
- 【図6】図5に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。
- 【図7】積分回路のさらに別の例を示す回路図である。
- 【図8】図7に示す積分回路を用いた物理乱数発生器の動作波形を示す図である。
- 【図9】本発明に係る物理乱数発生装置の一実施形態を示す回路図である。

## 【符号の説明】

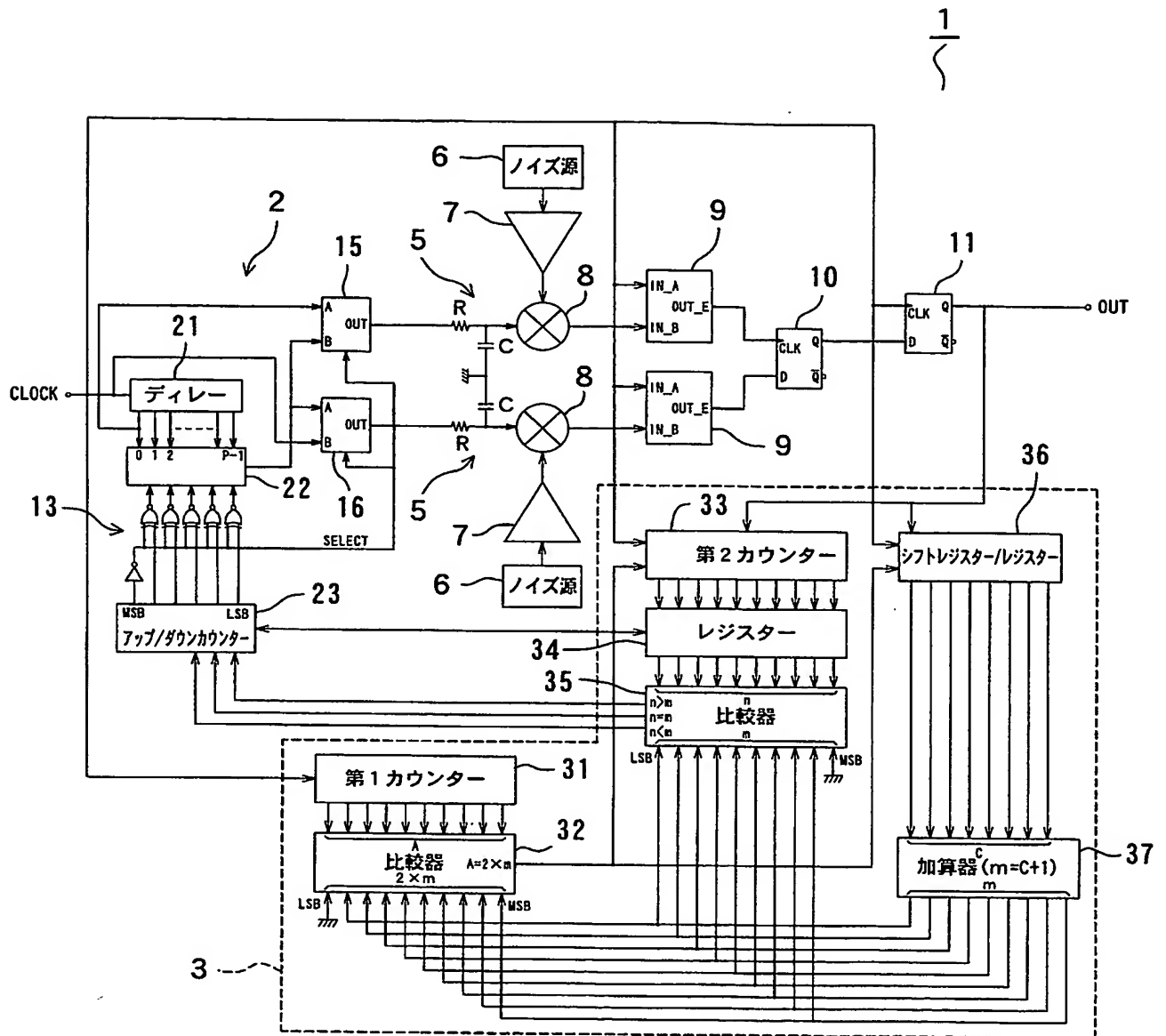
## 【0034】

- 1 ……物理乱数発生器
- 5 ……積分回路

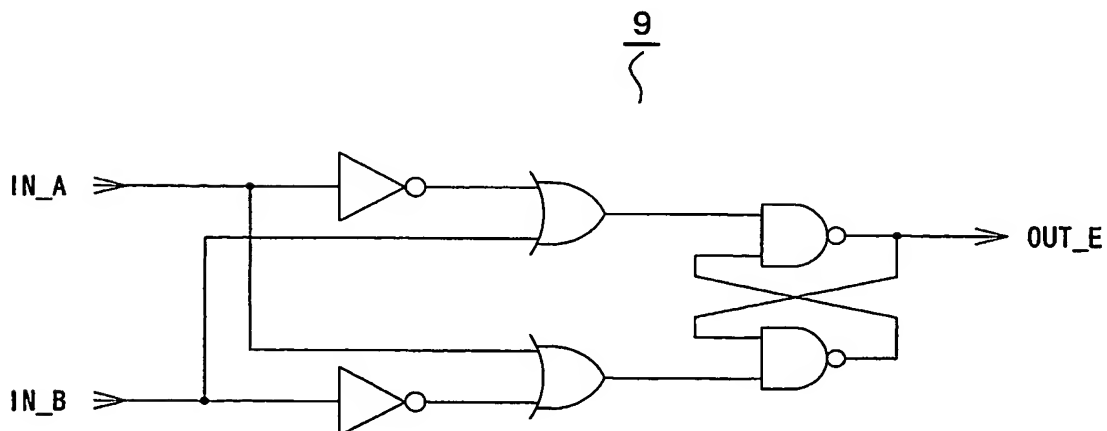


6 .....ノイズ源  
7 .....アンプ  
8 .....ミキサー  
9 .....エッジ検出回路  
1 0、1 1 .....フリップ・フロップ  
2 .....位相調整部  
1 5 .....第 2 セレクター  
1 6 .....第 3 セレクター  
2 1 .....ディレー  
2 2 .....第 1 セレクター  
2 3 .....アップ／ダウンカウンタ  
3 .....フィードバック回路  
1 7 .....F E T  
R .....抵抗  
C .....キャパシタ  
1 8 .....定電流回路

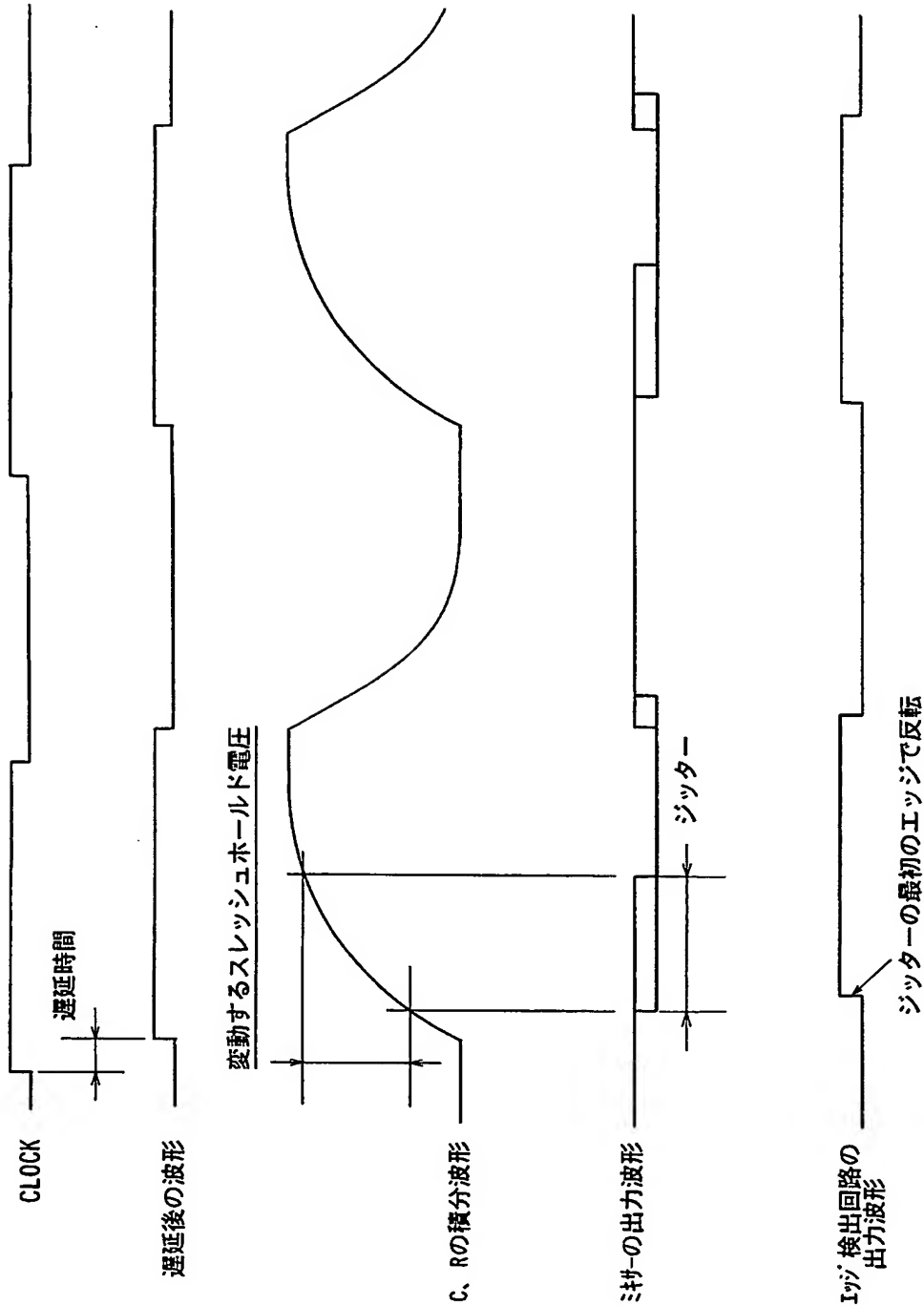
【書類名】 図面  
【図 1】



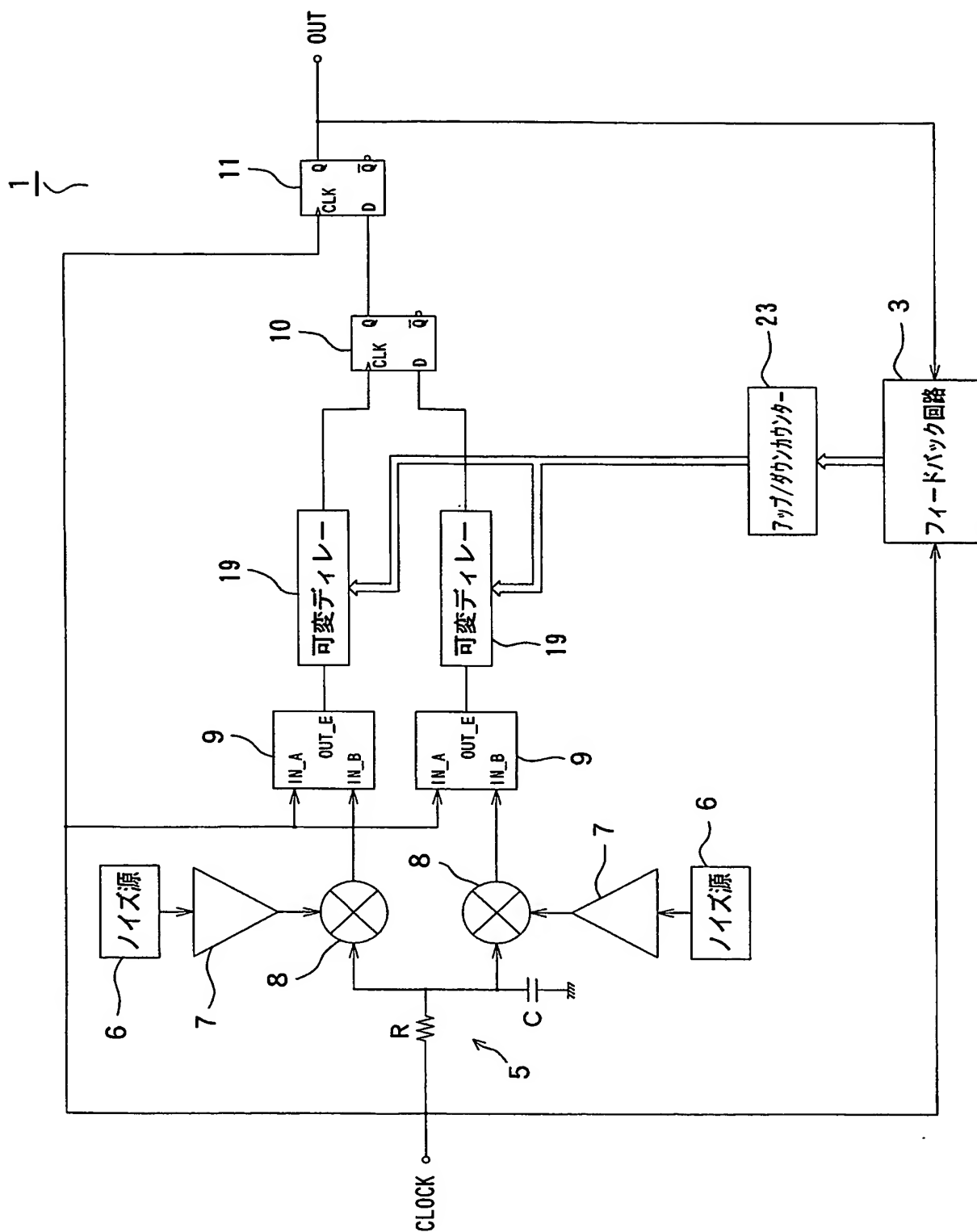
【図 2】



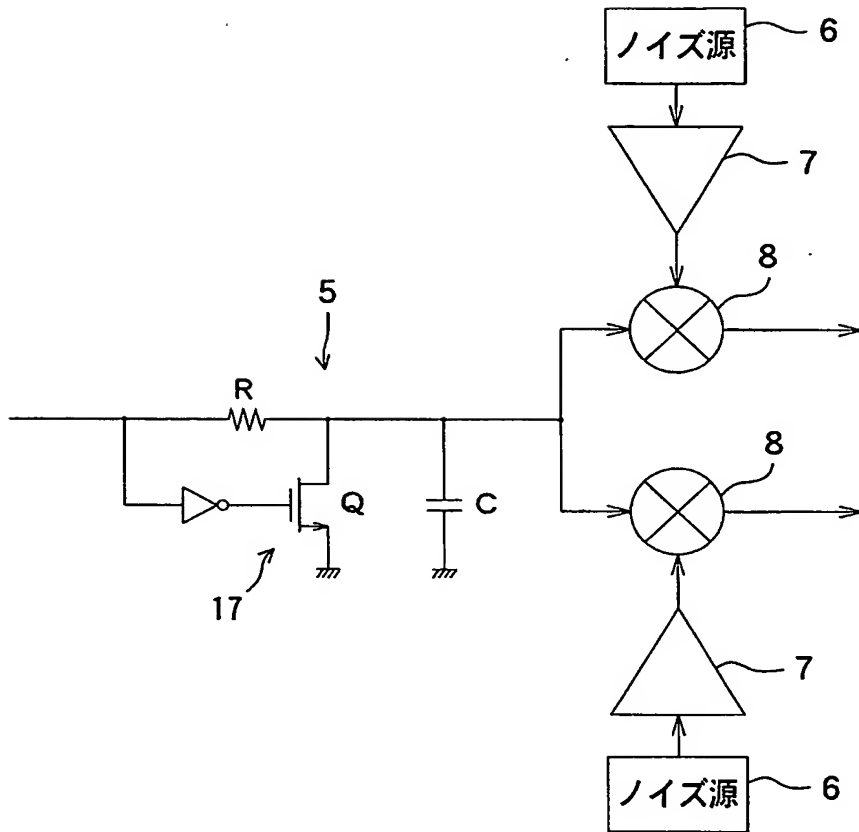
【図 3】



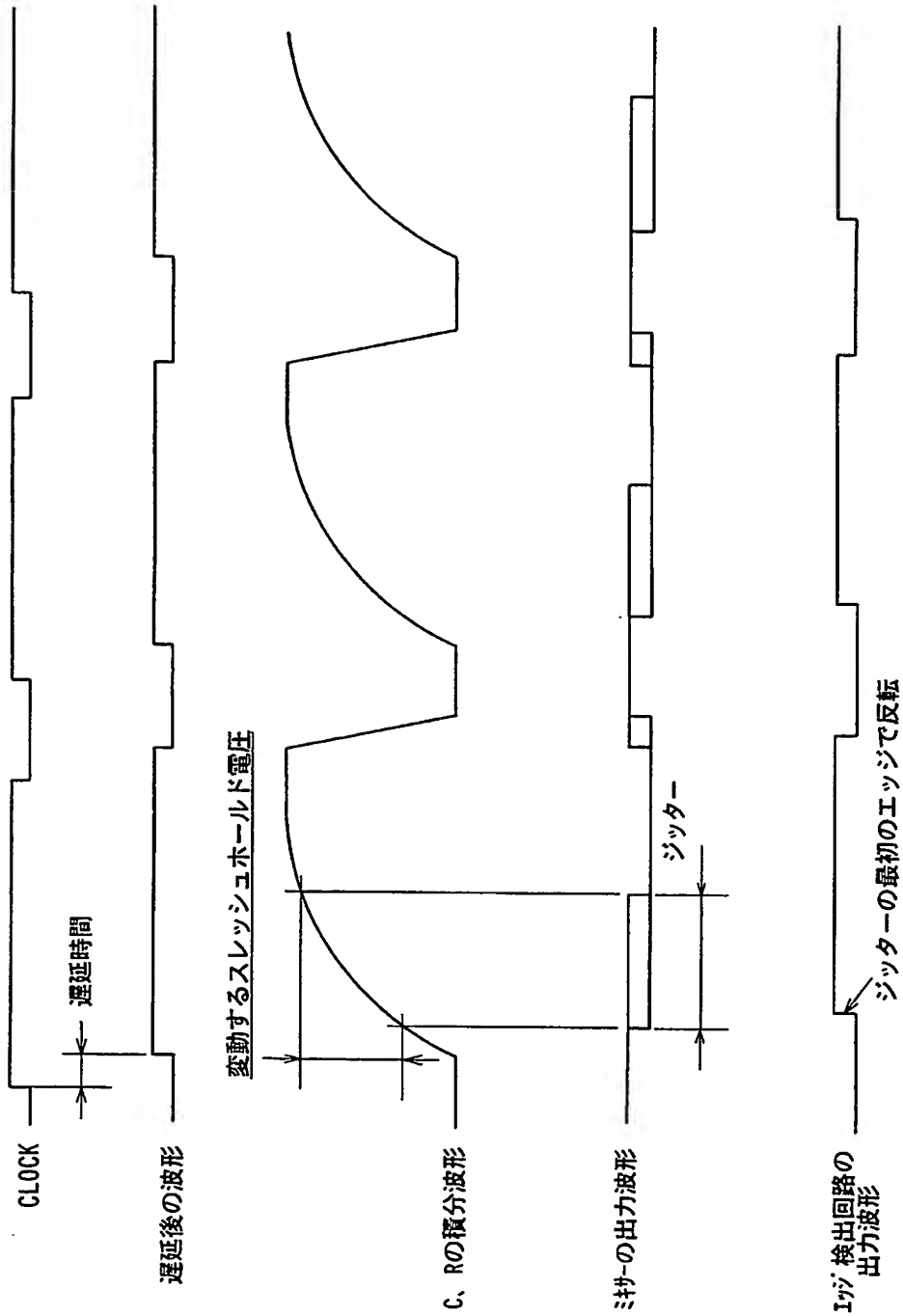
【図 4】



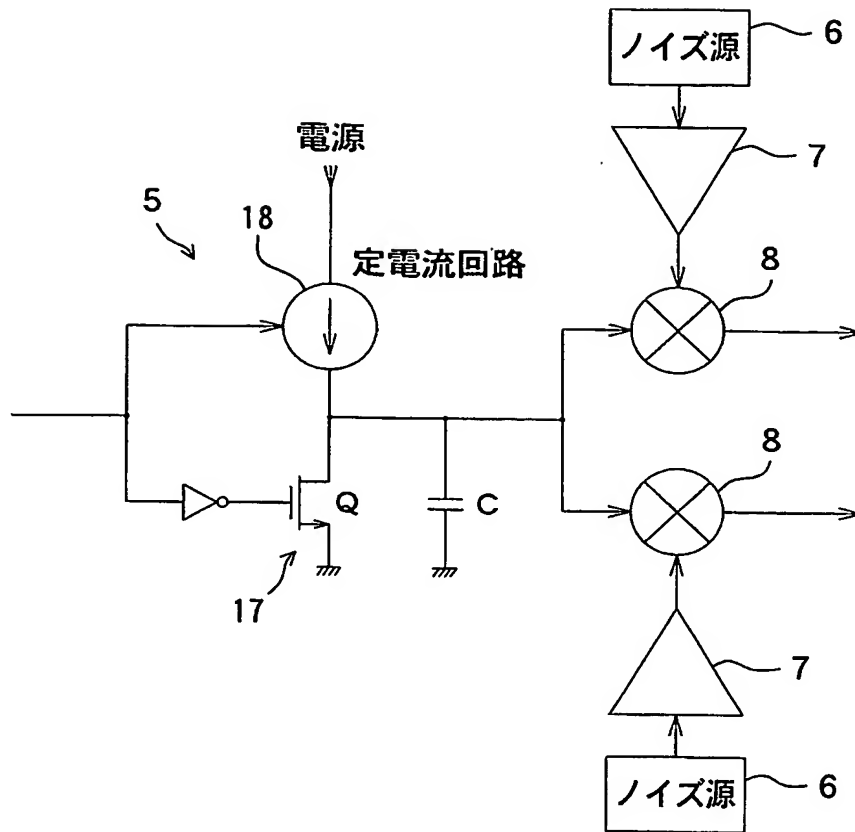
【図 5】



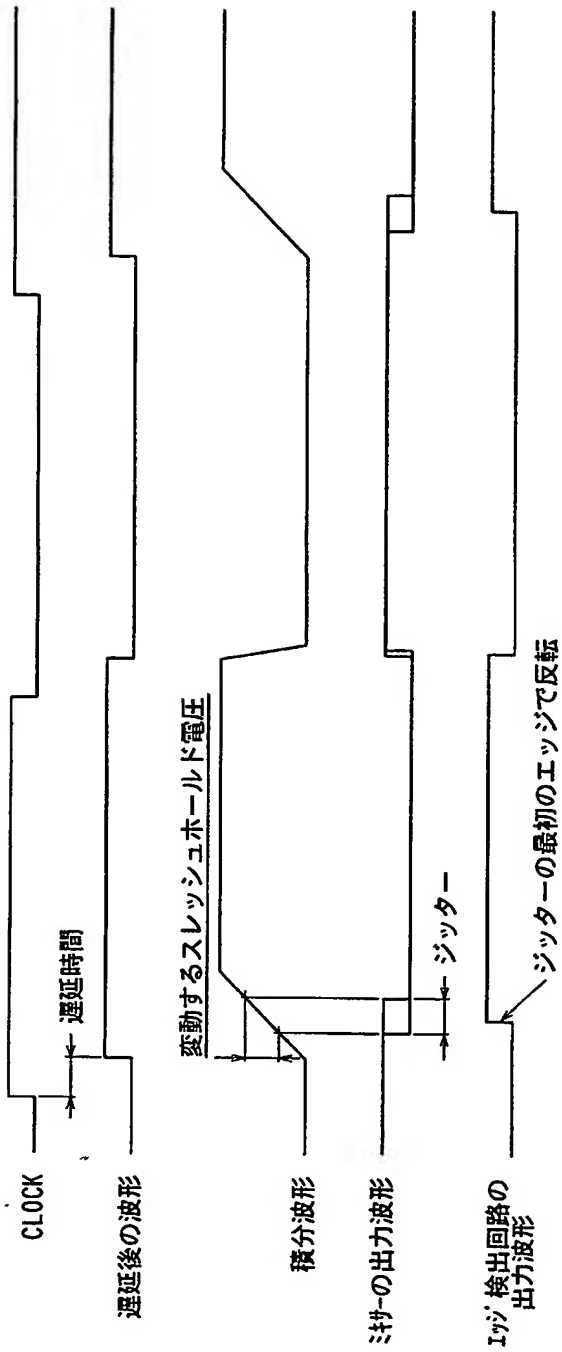
【図 6】



【図 7】

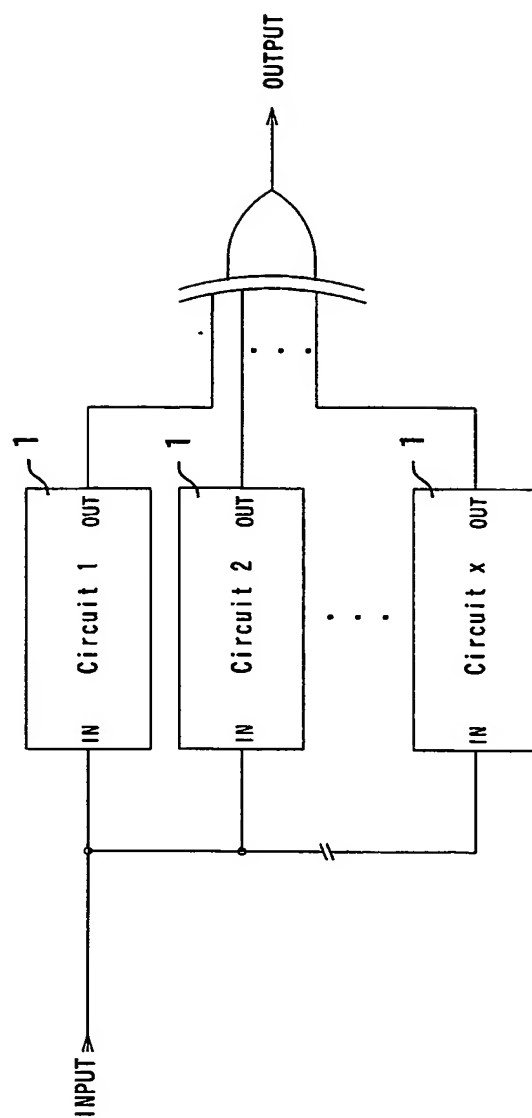


【図 8】





【図 9】



【書類名】要約書

【要約】

【課題】暗号化通信、ゲームなど各種の用途に用いるに好適な物理乱数発生器において、占有面積を縮小し、消費電力を低減する。

【解決手段】各積分回路 5 の前段にそれぞれ第 2 セレクター 1 5 および第 3 セレクター 1 6 を設け、アップ／ダウンカウンタ 2 3 の最上位ビットによって第 1 セレクター 2 2 と第 2 セレクター 1 5 および第 3 セレクター 1 6 との入力の極性切換を行う極性切換回路 1 3 を設ける。これにより、ディレー 2 1 および第 1 セレクター 2 2 を半分にしてゲート数を削減できる。また、積分回路 5 の抵抗 R の後段に F E T をキャパシタ C と並列に付加すれば、乱数の質が向上し、動作スピードが高速になる。さらに、積分回路 5 の抵抗 R に代えて定電流回路を設けると、乱数の質が向上する。

【選択図】図 1

認定・付加情報

特許出願の番号	特願 2003-294101
受付番号	50301352928
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年 8月19日

<認定情報・付加情報>

【提出日】 平成15年 8月18日

特願 2 0 0 3 - 2 9 4 1 0 1

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 2 3 7 7 2 1 ]

- |          |                          |
|----------|--------------------------|
| 1. 変更年月日 | 2 0 0 1 年   1 月 1 6 日    |
| [変更理由]   | 名称変更                     |
| 住 所      | 東京都港区新橋 5 丁目 3 6 番 1 1 号 |
| 氏 名      | エフ・ディー・ケイ株式会社            |
|          |                          |
| 2. 変更年月日 | 2 0 0 3 年   8 月 1 3 日    |
| [変更理由]   | 名称変更                     |
| 住 所      | 東京都港区新橋 5 丁目 3 6 番 1 1 号 |
| 氏 名      | F D K 株式会社               |